成分がRDSである一般アダマール行列の構成 (代数的組合せ論および関連する群と代数)

AUTHOR(S):

平峰, 豊

CITATION:

平峰, 豊. 成分がRDSである一般アダマール行列の構成 (代数的組合せ論および関連する群と代数). 数理解析研究所講究録 2010, 1687: 139-147

ISSUE DATE:

2010-05

URL:

http://hdl.handle.net/2433/141482

数理解析研究所講究録
第1687巻 2010年 139-147

成分がRDSである一般アダマール行列の構成

熊本大学・教育学部　平峰 豊 (Yutaka Hiramine)
Faculty of Education, Kumamoto University

1 Introduction

群 G の元を成分とする行列を用いて一般アダマール行列が定義されて，それにより symmetric transversal design が得られる ([1]). これに対して 変形一般アダマール行列は群環の元を成分として行列が定義されて，それを用いることにより 非対称な場合を含めて transversal design が得られる ([4]).

ここでは，さらに少し異なる視点から一般アダマール行列を一般化して変形一般アダマール行列の構成に利用することを考える. すなわち，一般アダマール行列では与えられた群 U の元を成分としてもつ行列 $[d_{ij}]$ が任意の異なる2行 i,j に対して $(*)$ $\sum_t d_{it}{d_{jt}}^{-1} = \lambda U$ を満たすように定められているが，この研究では少しゆるやかにして，d_{ij} を U を正規部分群として持つ群 G の元でよいとしてその代わり $(*)$ が U の剰余類の和集合であることを条件として課す (ただし，群環 $\mathbb{Z}[G]$ の元に対して $(\sum_{g\in G} a_g g)^{(-1)} = \sum_{g\in G} a_g g^{-1}$). これにより変形一般アダマール行列の新しい構成方法が与えるられる (Theorem 4.1, Theorem 4.7).

2 変形一般アダマール行列

最初に [4] の結果のうち後半で用いるものについてまとめる.

GH(s,u,λ) の定義

Definition 2.1. G を位数 su の群とする. G の s-部分集合 D_{ij} $(1 \leq i,j \leq t, st = u\lambda)$ に対して，次の行列

$$[D_{ij}] = \begin{bmatrix} D_{11} & D_{12} & \cdots & D_{1t} \\ D_{21} & D_{22} & \cdots & D_{2t} \\ \vdots & \cdots & \cdots & \vdots \\ D_{t1} & D_{t2} & \cdots & D_{tt} \end{bmatrix}$$

が G の位数 u の部分群 $U_1,\cdots,U_t$ に関する G 上の変形一般アダマール行列 (a GH(s,u,λ) matrix over G relative to $U_1,\cdots,U_t$, $k := u\lambda = st$) であると

は次の条件をみたすことをいう.

$$\sum_{1\le j\le t} D_{ij}D_{\ell j}{}^{(-1)} = \begin{cases} k+\lambda(G-U_i) & i=\ell \text{ のとき,} \\ \lambda G & i\neq \ell \text{ のとき.} \end{cases} \tag{1}$$

GH(s,u,λ) による $\mathbb{P}$ と $\mathbb{B}$ の定義

群環 $\mathbb{Z}[G]$ に成分をもつ t 次正方行列の全体を $\mathrm{M}_t(\mathbb{Z}[G])$ で表す.
GH(s,u,λ)-行列 $[D_{ij}]\in \mathrm{M}_t(\mathbb{Z}[G])$ relative to $U_1,\cdots,U_t$ $(t=u\lambda/s)$ に対して点集合 $\mathbb{P}$ とブロック集合 $\mathbb{B}$ を次で定める.

$$\mathbb{P} = \{1,2,\cdots,t\}\times G, \tag{2}$$

$$\mathbb{B} = \{B_{jh} : 1\le j\le t,\ h\in G\}, \tag{3}$$

ここで

$$B_{jh} = \bigcup_{1\le i\le t} (i, D_{ij}h)$$

G の元 x の点 $(i,g)\in\mathbb{P}$ への作用を $(i,g)x=(i,gx)$ で定義するとき, 次が成り立つ.

Result 2.2. ([4]) 位数 su の群 G に対して $[D_{ij}]\in \mathrm{M}_t(\mathbb{Z}[G])$ を位数 u の部分群 $U_1,\cdots,U_t$ $(t=u\lambda/s)$ に関する GH(s,u,λ)-行列とする. $\mathbb{P}$ と $\mathbb{B}$ を (2)(3) により定めるとき次が成り立つ.

(i) $(\mathbb{P},\mathbb{B})$ は $\mathrm{TD}_\lambda(k,u)$ $(k=u\lambda)$ である.

(ii) $G\le \mathrm{Aut}((\mathbb{P},\mathbb{B}))$ で, G は $\mathbb{P}$ と $\mathbb{B}$ 上に半正則に作用して任意の点軌道は s 個の点クラスの和集合である.

このことから, $GH(s,u,\lambda)$ を構成することにより transversal design が得られることが分かる. この研究では新しい $GH(s,u,\lambda)$ の構成法を述べる. $GH(s,u,\lambda)$ から得られる transversal design は必ずしも symmetric ではない. 次はその判定基準を与える.

STD に対応する GH(s,u,λ)-行列の判定法

Result 2.3. ([4]) su の群 H に対して $[D_{ij}]\in \mathrm{M}_t(\mathbb{Z}[H])$ を位数 u の部分群 $U_1,\cdots,U_t$ $(t=u\lambda/s)$ に関する GH(s,u,λ)-行列とする. このとき $[D_{ij}]$ に対応する $\mathrm{TD}_\lambda(k,u)$ が symmetric であるための必要十分条件は

$$[D_{ij}{}^{(-1)}]^T = \begin{bmatrix} D_{11}{}^{(-1)} & D_{21}{}^{(-1)} & \cdots & D_{t1}{}^{(-1)} \\ D_{12}{}^{(-1)} & D_{22}{}^{(-1)} & \cdots & D_{t2}{}^{(-1)} \\ \vdots & \cdots & \cdots & \vdots \\ D_{1t}{}^{(-1)} & D_{2t}{}^{(-1)} & \cdots & D_{tt}{}^{(-1)} \end{bmatrix}$$

が H の適当な部分群 $V_1,\cdots,V_t$ に関する GH(s,u,λ)-行列となることである.

次はアーベル群の指標に関するよく知られた結果である.

Result 2.4. ([7]) G がアーベル群で $f \in \mathbb{Z}[G]$ とする. G の単位指標 χ_0 とは異なるすべての指標 $\chi \in G^*$ に対して $\chi(z) = 0$ ならば $f = \lambda G$ $(\exists \lambda \in \mathbb{Z})$ である.

次は Result 2.4 の一般化である.

Lemma 2.5. U がアーベル群 G の部分群で, $z \in \mathbb{Z}[G]$ とする. $\chi_{|U} \neq \chi_0$ である任意の指標 $\chi \in G^*$ $(\chi \neq \chi_0)$ に対して常に $\chi(z) = 0$ であれば, $f \in \mathbb{Z}[G]$ が存在して $z = Uf$ と表される.

(証明) 仮定より $\chi(z(U-u)) = 0$ $(\forall \chi \in G^*,\ \chi \neq \chi_0)$. Result 2.4 を適用して $z(U-u) = sG$ となる整数 s が存在する. 両辺に単位指標を作用させて $s = 0$ が分かる. これより $zU = uz$. ここで G/U の完全代表系を $\{g_1, \cdots, g_m\}$ $(m = [G : U])$ とおくと, $z = g_1w_1 + g_2w_2 + \cdots + g_mw_m$ $(\exists w_1, \cdots, w_m \in \mathbb{Z}[U])$ とおけるから $(g_1w_1 + g_2w_2 + \cdots + g_mw_m)U = u(g_1w_1 + g_2w_2 + \cdots + g_mw_m)$. 従って

$$g_1\chi_0(w_1)U + \cdots + g_m\chi_0(w_m)U = g_1uw_1 + \cdots + g_muw_m \tag{4}$$

(4) の $g_1, \cdots, g_m$ の係数を比較して,

$$\chi_0(w_i)U = uw_i, \qquad (1 \leq i \leq m) \tag{5}$$

ここで $U = \{x_1, \cdots, x_u\}$ とおけば $w_i = a_{i1}x_1 + \cdots + a_{iu}x_u$ $(\exists a_1, \cdots, a_u \in \mathbb{Z})$ の形に表されるので, (5) に代入して $x_1, \cdots, x_u$ の係数を比較すれば次を得る.

$$(a_{i1} + \cdots + a_{iu}) \sum_{1 \leq j \leq u} x_j = \sum_{1 \leq j \leq u} a_{ij}ux_j$$

これより $a_{i1} + \cdots + a_{iu} = a_{i1}u = \cdots = a_{iu}u$. よって $a_{i1} = \cdots = a_{iu}$ がわかるので $w_i = s_iU$ $(\exists s_i \in \mathbb{Z})$. 以上より Lemma が成り立つ.

3 Cosets N/U に関する一般アダマール行列

この節では Definition 2.1 とは別の視点から一般アダマール行列の拡張を行って, 次の節でそれを変形一般アダマール行列の構成に利用する.

Definition 3.1. N を群, U をその正規部分群として $N/U = \{U_1(= U), U_2, \cdots, U_m\}$(剰余類分解) とおく. このとき, n 次正方行列 $H = [h_{ij}]$ が N/U に関する一般アダマール行列 $\mathrm{GH}(u, \lambda)$ ($\mathrm{GH}(u, \lambda)$-matrix with respect to N/U) であるとは $n = u\lambda$ で,

(i) $h_{ij} \in N$ $(1 \leq i, j \leq n)$ 及び

(ii) 任意の i,j,t $(1 \leq i \neq j \leq n,\ 1 \leq t \leq m)$ に対して $\lambda_{ijt} \geq 0$ が存在して

$$\sum_{1 \leq t \leq n} h_{it}h_{jt}^{-1} = \lambda_{ij1}U_1 + \cdots + \lambda_{ijm}U_m$$

つまり

$$H(H^{(-1)})^T = \begin{bmatrix} n & Uz_{12} & \cdots & Uz_{1n} \\ Uz_{21} & n & & \\ \vdots & & \cdots & \\ Uz_{n1} & \cdots & & n \end{bmatrix}$$

ここで $z_{ij} \in \mathbb{Z}[N]$ かつ z_{ij} の係数はすべて 0 以上で N の単位指標 χ_0 に対して $\chi_0(z_{ij}) = \lambda$

をみたすことをいう.

Remark 3.2. (1) 群 U 上の通常の GH(u,λ)-行列は U/U に関する GH(u,λ)-行列と見ることができる.

(2) $u\lambda = (\lambda_{ij1} + \cdots + \lambda_{ijm})|U|$ $(\forall i,j)$ により, すべての i,j $(i \neq j)$ について次がみたされていなければならない.

$$\lambda = \lambda_{ij1} + \cdots + \lambda_{ijm}$$

Example 3.3. $N = \langle a \rangle \simeq \mathbb{Z}_4$, $U = \langle a^2 \rangle \simeq \mathbb{Z}_2$, $U_1 = U, U_2 = Ua$ とする. N の元を成分とする次の 4 次正方行列 $M = [d_{ij}]$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & a^2 & a^2 \\ 1 & a^2 & a & a^3 \\ 1 & a^2 & a^3 & a \end{bmatrix}$$

は任意の i,j $(i \neq j)$ に対して $\sum_{1 \leq t \leq 4} d_{it}d_{jt}^{-1}$ が $cU_1 + dU_2$ $(c,d \geq 0)$ の形であることが確かめられるので, GH(2,2)-行列 w.r.t N/U である.

Example 3.4. $N = \langle a \rangle \simeq \mathbb{Z}_9$, $U = \langle a^3 \rangle \simeq \mathbb{Z}_3$ とすると $N/U = \{U(= \{1, a^3, a^6\}),\ Ua(= \{a, a^4, a^7\}),\ Ua^2(= \{a^2, a^5, a^8\})\}$(剰余類分解) である. このとき,

$$[h_{ij}] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 \\ 1 & a^4 & a^8 & a^3 & a^7 & a^2 & a^6 & a & a^5 \\ 1 & a^7 & a^5 & a^3 & a & a^8 & a^6 & a^4 & a^2 \\ 1 & 1 & 1 & a^6 & a^6 & a^6 & a^3 & a^3 & a^3 \\ 1 & a^3 & a^6 & 1 & a^3 & a^6 & 1 & a^3 & a^6 \\ 1 & a^3 & a^6 & a^6 & 1 & a^3 & a^3 & a^6 & 1 \\ 1 & a^6 & a^3 & 1 & a^6 & a^3 & 1 & a^6 & a^3 \\ 1 & a^6 & a^3 & a^6 & a^3 & 1 & a^3 & 1 & a^6 \end{bmatrix}$$

は一般アダマール行列 GH(3,3) w.r.t N/U である.

Example 3.5. $N=\langle a\rangle \simeq \mathbb{Z}_6 \geq U=\langle a^2\rangle \simeq \mathbb{Z}_3$ に対して
$N/U=\{U(=\{1,a^2,a^4\}),\ Ua(=\{a,a^3,a^5\})$ とおく.
このとき

$$[h_{ij}]=\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
1 & 1 & a & a^2 & a^4 & a^4 & a^5 & 1 & a^2 & a^2 & a^3 & a^4\\
1 & 1 & a^4 & a^2 & 1 & a^2 & a^4 & a^2 & 1 & a^4 & a^4 & a^2\\
1 & 1 & a^2 & a^4 & 1 & a^2 & a^2 & a^4 & a^4 & 1 & a^2 & a^4\\
1 & a^4 & a & 1 & a^2 & a^3 & a & a^2 & a^5 & a^3 & a^5 & a^4\\
1 & a^4 & a^3 & a^4 & a^2 & a^5 & a & 1 & a & a^5 & a^3 & a^2\\
1 & a^4 & a^3 & a^2 & a^2 & a & a^5 & a^4 & a^3 & a & a^5 & 1\\
1 & a^4 & a^5 & a^4 & 1 & a^4 & a^3 & a^2 & a^2 & a^2 & a & 1\\
1 & a^2 & a^5 & a^2 & a^2 & 1 & a^3 & 1 & a^4 & a^4 & a & a^4\\
1 & a^2 & a^3 & 1 & a^4 & a^4 & a^5 & a^2 & a^4 & 1 & a & a^2\\
1 & a^2 & a & a^4 & a^4 & 1 & a^3 & a^4 & 1 & a^2 & a^5 & a^2\\
1 & a^2 & a^5 & 1 & a^4 & a^2 & a & a^4 & a^2 & a^4 & a^3 & 1
\end{bmatrix}$$

は $\sum_{1\leq t\leq 12} h_{it}{h_{jt}}^{-1}\in\{4U,3U+Ua,2U+2Ua\}$ であることが確かめられて, GH(3,4)-行列 w.r.t. N/U である.

Kronecker 積の定義から次が容易に確かめられる.

Proposition 3.6. U を群 N の正規部分群として $H_i(i=1,2)$ が N/U に関する一般アダマール行列 $\mathrm{GH}(u,\lambda_i)$ ならば $H_1\otimes H_2$ も N/U に関する一般アダマール行列 $\mathrm{GH}(u,\lambda_1\lambda_2 u)$ である.

4 Cosets N/U に関する一般アダマール行列 と RDS

この節では N/U に関する一般アダマール行列と群 $G(\geq N)$ における半正則相対差集合 (semiregular RDS relative to U) を用いて変形一般アダマール行列が構成できることを示し, さらにその例を示す.

Theorem 4.1. G を位数 $u^2\mu$ の群, U を G の位数 u の部分群で $N(\geq U)$ を $N_G(U)$ の部分群とする. $H=[h_{ij}])$ を N/U に関する $\mathrm{GH}(u,\lambda)$-行列で, $\mathcal{D}=(D_1,D_2,\cdots,D_n)$ $(n=u\lambda)$ を G の $(u\mu,u,u\mu,\mu)$-RDSs relative to U の任意の n-tuple とする. このとき n 次正方行列

$$M_{H,\mathcal{D}}=\begin{bmatrix}
h_{11}D_1 & h_{12}D_2 & \cdots & h_{1n}D_n\\
h_{21}D_1 & h_{22}D_2 & \cdots & h_{2n}D_n\\
\vdots & \vdots & & \vdots\\
h_{n1}D_1 & h_{n2}D_2 & \cdots & h_{nn}D_n
\end{bmatrix} \tag{6}$$

は U に関する変形一般アダマール行列 $\mathrm{GH}(u\mu,u,u\lambda\mu)$ である.

(証明) $N/U = \{U_1(=U), U_2, \cdots, U_m\}$ (剰余類分解) とおくと，仮定より任意の i, j $(i \neq j)$ に対して $\lambda_{ijk} \geq 0$ $(1 \leq i, j \leq n,\ 1 \leq k \leq m)$ があって次を満たす.

$$\sum_{1 \leq t \leq n} h_{it} {h_{jt}}^{-1} = \lambda_{ij1} U_1 + \lambda_{ij2} U_2 + \cdots + \lambda_{ijm} U_m \tag{7}$$

$$n = (\lambda_{ij1} + \cdots + \lambda_{ijm}) u \tag{8}$$

また，$D_{ij} = d_{ij} D_j$ とおけば $M_{H,\mathcal{D}} = [D_{ij}]$.

$i \neq j$ のとき，(7), (8) と $N \triangleright U$ を用いれば，

$\sum_{1 \leq t \leq n} D_{it} {D_{jt}}^{(-1)} = \sum_{1 \leq t \leq n} h_{it} (u\mu + \mu(G - U)) {h_{jt}}^{-1}$

$\sum_{1 \leq t \leq n} h_{it} {h_{jt}}^{-1} (u\mu + \mu(G - U)) = \sum_{1 \leq k \leq m} \lambda_{ijk} U_k (u\mu + \mu(G - U))$

$= u\mu \sum_{1 \leq k \leq m} \lambda_{ijk} U_k + \mu(\sum_{1 \leq k \leq m} \lambda_{ijk} |U_k|) G - \mu \sum_{1 \leq k \leq m} \lambda_{ijk} |U| U_k$

$= \mu(\sum_{1 \leq k \leq m} \lambda_{ijk} u) G = \mu n G.$

一方 $i = j$ のとき，$\sum_{1 \leq t \leq n} D_{it} {D_{it}}^{(-1)} = \sum_{1 \leq t \leq n} h_{it} (u\mu + \mu(G - U) {h_{it}}^{-1}$

$= (u\mu + \mu(G - U)) = nu\mu + n\mu(G - U).$

これより

$$\sum_{1 \leq t \leq n} D_{it} {D_{jt}}^{(-1)} = \begin{cases} nu\mu + n\mu(G - U) & i = j \text{ のとき}, \\ n\mu G & i \neq j \text{ のとき} \end{cases}$$

従って定理が成り立つ. □

Corollary 4.2. G を位数 $u^2\mu$ の群，U を G の位数 u の正規部分群とする．$H = [h_{ij}]$ を G/U に関する GH(u, λ)-行列で，$\mathcal{D} = (D_1, D_2, \cdots, D_n)(n = u\lambda)$ を G の $(u\mu, u, u\mu, \mu)$-RDSs relative to U の n-tuple とする．このとき (6) で定義される n 次正方行列は U に関する変形一般アダマール行列 GH$(u\mu, u, u\lambda\mu)$ である.

Example 4.3. $G = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$. $H = [h_{ij}]$ を $U = \langle a \rangle$ に成分を持つ次の GH$(3, 1)$-行列とする.

$$H = \begin{bmatrix} a & 1 & 1 \\ 1 & a & 1 \\ 1 & 1 & a \end{bmatrix}$$

また，$D_t = \{a^i b^{i^2+t} : i \in \mathbb{Z}_3\}$ $(1 \leq t \leq 3)$ とおくと D_t は G の $(3, 3, 3, 1)$-RDS. 従って，$\mathcal{D} = (D_1, D_2, D_3)$ に対して $M_{H,\mathcal{D}} = \begin{bmatrix} aD_1 & D_2 & D_3 \\ D_1 & aD_2 & D_3 \\ D_1 & D_2 & aD_3 \end{bmatrix}$ は Cor. 4.2 より GH$(3, 3, 3)$-行列 relative to $\langle a \rangle$ である.

Example 4.4. $G = \langle r, s \rangle \times \langle t \rangle \simeq Sym(3) \times \mathbb{Z}_6$ $(r^2 = s^3 = t^6 = 1, [r, t] = [s, t] = 1, rsr = s^{-1})$ とする. [3] により

$$D=\{1,t,t^2,t^3,r,rt,s,r^2st^5,rst^4,r^2st,st^4,rst\}$$

は non-normal $(12,3,12,4)$-RDS in G relative to $U=\langle rt^2\rangle$ の1つである. $\mathcal{D}=(D_1,\cdots,D_{12})$ $(12,3,12,4)$-RDSs in G relative to U の任意の 12-tuple とする. さらに, $N=\langle rt^{-1}\rangle\simeq\mathbb{Z}_6\supset U=\langle rt^2\rangle\simeq\mathbb{Z}_3$ であるから, N は Example 3.5 における GH$(3,4)$-行列 w.r.t. N/U をもつ. これを $H=[h_{ij}]$ としておくと Theorem 4.1 より $M_{H,\mathcal{D}}$ は GH$(12,3,48)$-行列 (relative to U) でありこれより TD$_{48}(144,3)$ を得る.

Lemma 4.5. Theorem 4.1 において G がアーベル群のとき, $M_{H,\mathcal{D}}$ が定める TD$_{u\lambda\mu}(u^2\lambda\mu,u)$ が対称であるための必要十分条件は H^T が N/U に関する GH(u,λ)-行列となることである.

(証明) Result 2.3 より任意の j,ℓ $(1\le j\ne\ell\le n)$ に対して

$$\sum_{1\le s\le n}h_{sj}D_j(h_{s\ell}D_\ell)^{(-1)}=\mu nG$$

が成り立つことが必要十分である. このことから G の任意の指標 $\chi(\neq\chi_0)$ に対して $\chi(D_j)\overline{\chi(D_\ell)}\chi(\sum_{1\le s\le n}h_{sj}h_{s\ell}^{-1})=0$ が成り立つことが必要十分条件である. 一方, $i\in\{j,\ell\}$ に対して

$$|\chi(D_i)|^2=\chi(D_iD_i^{(-1)})=\chi(u\mu+\mu(G-U))=u\mu-\mu\chi(U)$$

であるから, $\chi(\sum_{1\le s\le n}h_{sj}h_{s\ell}^{-1})=0$ が $\chi_{|U}\ne\chi_0$ なる指標 χ について成り立つことが必要十分である. 補題2.5よりこれは H^T が G/U に関する GH(u,λ)-行列となることと同値である. 従って命題が成り立つ. □

Example 4.6. $N=\langle a\rangle\simeq\mathbb{Z}_9\supset U=\langle a^3\rangle\simeq\mathbb{Z}_3$ で, $H=[h_{ij}]$ を例 3.4 の一般アダマール行列 GH$(3,3)$ w.r.t N/U とする. $G=\langle a\rangle\times\langle b\rangle\simeq\mathbb{Z}_9\times\mathbb{Z}_3$ には $(9,3,9,3)$-RDS relative to U が存在する ([6]) から重複を許してそれを 9 個選んで $\mathcal{D}=(D_1,\cdots,D_9)$ とする. このとき Theorem 4.1 より $M_{H,\mathcal{D}}$ は G における変形一般アダマール行列 GH$(9,3,27)$ relative to U であるが, H^T も一般アダマール行列 GH$(3,3)$ w.r.t N/U であることがチェックできるので Lemma 4.5 より $M_{H,\mathcal{D}}$ から得られる TD$_{27}(81,3)$ は symmetric である.

D が群 G における $(u\mu,u,u\mu,\mu)$-RDS relative to U であれば定義より D は G における U の右代表系であるが一般には左代表系ではない. しかし D がもし左代表系でもあれば次が成り立つ.

Theorem 4.7. G を位数 $u^2\mu$ の群, U を G の位数 u の部分群, $N(\ge U)$ を $N_G(U)$ の部分群とする. また, $H=[h_{ij}]$ $(h_{ij}\in N)$ を N/U に関する GH(u,λ)-行列で $\mathcal{D}=(D_1,D_2,\cdots,D_n)$ $(n=u\lambda)$ を G の $(u\mu,u,u\mu,\mu)$-RDSs relative to U の n-tuple で, $\mathcal{D}$ のうち少なくとも $n-1$ 個が G における U の

左代表系であるとする．このとき n 次正方行列

$$M'_{H,\mathcal{D}} = \begin{bmatrix} D_1h_{11} & D_1h_{12} & \cdots & D_1h_{1n} \\ D_2h_{21} & D_2h_{22} & \cdots & D_2h_{2n} \\ \vdots & \vdots & & \vdots \\ D_nh_{n1} & D_nh_{n2} & \cdots & D_nh_{nn} \end{bmatrix} \tag{9}$$

は U に関する変形一般アダマール行列 $\mathrm{GH}(u\mu, u, u\lambda\mu)$ relative to U である．

(証明) $N/U = Ug_1 \cup \cdots \cup Ug_m (g_1, \cdots, g_m \in N)$ (剰余類分解) とおく．このとき，仮定より

$$\sum_{1\le t\le n} h_{it}h_{jt}^{-1} = \lambda_{ij1}Ug_1 + \cdots + \lambda_{ijm}Ug_m \tag{10}$$

$D_{ij} = D_ih_{ij}$ とおけば $M'_{H,\mathcal{D}} = [D_{ij}]$．このとき，(10) を用いて

$$\begin{aligned} \sum_{1\le t\le n} D_{it}D_{jt}{}^{(-1)} &= \sum_{1\le t\le n} D_ih_{it}h_{jt}^{-1}D_j^{(-1)} = D_i(\sum_{1\le t\le n} h_{it}h_{jt}^{-1})D_j^{(-1)} \\ &= \begin{cases} D_i(\lambda_{ij1}Ug_1 + \cdots + \lambda_{ijm}Ug_m)D_j^{(-1)} & (i \ne j \text{ のとき}) \\ n(u\mu + \mu(G-U) & (i = j \text{ のとき}) \end{cases} \end{aligned}$$

$i \ne j$ のとき，仮定より $D_iU = G$ または $UD_j^{(-1)} = G$ が成り立つことに注意すれば $\sum_{1\le t\le n} D_{it}D_{jt}{}^{(-1)} = \lambda u\mu G$．以上より

$$\sum_{1\le t\le n} D_{it}D_{jt}{}^{(-1)} = \begin{cases} nu\mu + n\mu(G-U) & i = j \text{ のとき}, \\ n\mu G & i \ne j \text{ のとき} \end{cases}$$

従って定理が成り立つ．　□

Corollary 4.8. G を位数 $u^2\mu$ の群，U を G の位数 u の正規部分群とする．また，$H = [h_{ij}]$ を $\mathrm{GH}(u, \lambda)$-行列 w.r.t. G/U で $\mathcal{D} = (D_1, D_2, \cdots, D_n)$ $(n = u\lambda)$ を G の $(u\mu, u, u\mu, \mu)$-RDSs relative to U の n-tuple であるとする．このとき (9) で定義される n 次正方行列は U に関する変形一般アダマール行列 $\mathrm{GH}(u\mu, u, u\lambda\mu)$ である．

Example 4.9. 位数 $4n^2$ の形のアーベル群 L において多くの $(4n^2, 2n^2 - n, n^2 - n)$-差集合 A が構成されていて ([5]) Mennon Hadamard difference set と呼ばれている．このとき $G = L\langle t\rangle$ を t が L を invert する群として定義する．[2] の Proposition 4.14 と同様にして $D = A + (L - A^{(-1)})t$ は G における $(4n^2, 2, 4n^2, 2n^2)$-RDS relative to $U = \langle t\rangle$ となることが容易に証明できる．このうちで，spread 型の Mennon Hadamard difference set のように $A = A^{(-1)}$ を満たすものを考えて，さらに L は基本可換 2-群でないとする．$g \in L$ とすると Dg は G における $(4n^2, 2, 4n^2, 2n^2)$-RDS relative to U であ

るが，$(Dg)^{(-1)}(Dg) = 4n^2 + 2n^2(G - \langle gt \rangle)$ がなりたつので Dg は G における U の左代表系でない．また，$C_G(t)$ は $N = \langle t \rangle \times \langle s \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ なる群を含む．4 次の GH(2, 2)-行列 w.r.t N/U を $H = [h_{ij}]$ とする．例えば次を選ぶ．

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & t & s & st \\ 1 & 1 & t & t \\ 1 & t & st & s \end{bmatrix}$$

また，$\mathcal{D} = (D, D, D, Dg)$ とすると Theorem 4.7 より $M'_{H,\mathcal{D}}$ は $GH(4n^2, 2, 8n^2)$-行列である．

Example 4.10. $F \simeq (GF(q), +)$ として $\begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \end{bmatrix}$ を GH$(q, 2)$ で各 $D_i (1 \leq i \leq 4)$ は GH$(q, 1)$ とする ([1] の Theorem 8.3.14 参照)．このとき $N = F \times \langle a \rangle$ $(a^2 = 1)$ とおけば $\begin{bmatrix} D_1 a & D_2 \\ D_3 & D_4 a \end{bmatrix}$ は GH$(q, 2)$ w.r.t. N/F である．

参考文献

[1] T. Beth, D. Jungnickel and H. Lenz, "Design Theory" Volume I, Second Edition, Cambridge University Press, 1999.

[2] A.D. Garciano, Y. Hiramine and T. Yokonuma, On Relative Difference Sets in Dihedral Groups, Designs, codes and Cryptography, Vol. 39, (2006) 51-63.

[3] Y. Hiramine, On non-symmetric relative difference sets, Hokkaido Mathematical Journal, Vol. 37 (2008) 427-435.

[4] Y. Hiramine, Modified generalized Hadamard matrices and constructions for transversal designs, to appear in Designs, Codes and Cryptography.

[5] E. S. Lander, *Symmetric Designs : An Algebraic Approach*, Lecture Note Sries 74, Cambridge University Press, Cambridge.

[6] S. L. Ma and A. Pott, Relative Difference Sets, Planar Functions, and Generalized Hadamard matrices, J. Algebra Vol. 175 (1995) 505-525.

[7] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics 1797, Springer-Verlag, Berlin Heiderberg (2002)